(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 October 2003 (02.10.2003)

PCT

(10) International Publication Number
WO 03/081934 A1

(51) International Patent Classification[7]: H04Q 7/38, H04L 9/32

(21) International Application Number: PCT/IB02/00911

(22) International Filing Date: 26 March 2002 (26.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; P.O. Box 226, FIN-00045 Nokia Group (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **HUSSMANN, Holger** [DE/FI]; Satakunnankatu 22, E125, FIN-33210 Tampere (FI).

(74) Agent: **AWAPATENT AB**; P.O. Box 5117, S-200 71 Malmö (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette

(54) Title: APPARATUS, METHOD AND SYSTEM FOR AUTHENTICATION

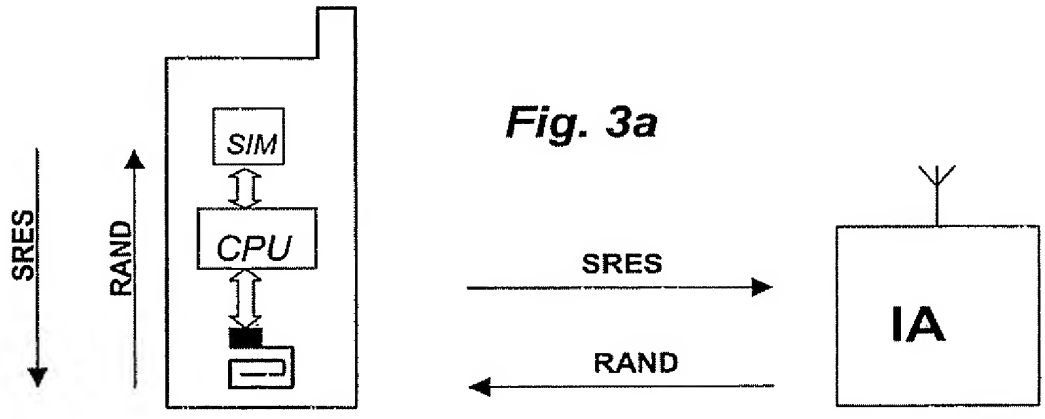


Fig. 3a

(57) Abstract: The invention relates to a portable, electronic device (201) such as a mobile phone. The device is provided with a transponder (202) and may be used for authentication purposes. The device includes means (204) for writing user-specific information into a memory unit (203), included in the transponder (202). Thus, when an interrogating reading device stimulates the transponder, the transponder emits the user-specific information. This enables authentication of a user rather than of a device. In a preferred embodiment use is made of a user-specific key, by means of which a single-use code is generated, which is used as the emitted user-specific information. The invention also relates to a method and a system, which may work in connection with such a device.

WO 03/081934 A1

APPARATUS, METHOD AND SYSTEM FOR AUTHENTICATION

Field of the invention

The invention relates to a portable, electronic device according to the preamble of claim 1, a method for use in an interrogating apparatus according to claim 10 and a system for authenticating a user according to the preamble of claim 13.

Technical background

RFID-transponders, sometimes referred to as RFID-tags (RFID=Radio Frequency Identification) are widely used for recognizing persons and objects.

An RFID-transponder may be devised as a small tag and carries stored information, such as an identity number, identifying an object or a person. In order to retrieve the stored information an interrogating apparatus is used. The apparatus emits an interrogating radio signal or field, which causes the RFID-transponder to reply with a signal, comprising the stored information. The interrogating apparatus may then receive the reply signal.

Such RFID transponders are used for instance in connection with access control or as an alternative to barcodes. In other common applications RFID transponders are used in car immobilisers and for identifying domestic animals.

It has been suggested to provide portable, electronic devices, such as mobile phones, with RFID transponders. This enables additional functionalities in connection with such devices. For instance, a mobile phone may then be used also as an access control card. Such functionalities often need strong security.

A problem with using such devices in this manner is that they are sometimes stolen, lost, sold or given away. Any access right or user registration given to the associated RFID transponder identity is then inherited by the new possessor of the device. This implies a lack of se-

curity, since the device may be misused, and makes - portable, electronic devices with RFID-transponders less credible.

Summary of the invention

One object of the present invention is to wholly or partly obviate the above-mentioned problems.

This object is achieved with a portable, electronic device as defined in claim 1, a method as defined in claim 10 and a system as defined in claim 13.

In accordance with a first aspect, the invention more specifically relates to a portable electronic device comprising a transponder with a memory unit. The device is characterised by means for writing user-specific information into the transponder memory unit, so that the transponder, upon receiving an interrogating signal, generates a response signal comprising the user-specific information.

In such a device the RFID-functionality is not statically tied to the device itself, but rather to the user of the device. This eliminates the problem associated with portable, electronic devices changing hands as described above.

Preferably, a portable, electronic device may comprise a detachable subscriber unit from which the user-specific information is retrieved. Such a unit may in the case of a GSM mobile phone be a SIM-unit, which then provides user-specific information which is independent of the phone used.

In a preferred embodiment the portable, electronic device comprises calculating means for calculating an authentication code, included in the user-specific information. This provides for the use of user-specific information that is used only once, thus providing improved credibility. If a detachable subscriber unit is used, the calculating means may preferably be located within this unit.

Preferably, the authentication code may be calculated based on a user-specific key a request code and using an algorithm. This allows excellent credibility and may be readily implemented in systems where such algorithms are used for other reasons, such as for instance in GSM-systems. Then the request code may preferably be comprised in the interrogating signal, received by the portable, electronic device.

In another embodiment, the user-specific information may be a user identity number, such as for instance an IMSI-number. This allows a simple way of performing authentication.

The portable, electronic device may preferably be a GSM mobile phone.

The transponder may preferably be intended to be used as an RFID-tag.

According to a second aspect, the invention relates to a method for use in an interrogating apparatus for authenticating a user, who is carrying a portable, electronic device, comprising a transponder with a memory unit. The method comprises the steps of: transmitting a transponder interrogating signal to the transponder of the portable device; receiving a response signal, comprising user specific information, from the transponder, said user-specific information being written, by means in the portable, electronic device, into a memory unit of the transponder; and determining the authenticity of the user based on the user-specific information.

Similarly to the above-mentioned device, this method provides reliable and user-oriented authentication.

Preferably in the method, the transponder interrogating signal comprises a request code, allowing the portable device to calculate an authentication code to be transmitted by the transponder, the calculation being based on the request code and a user-specific key and using an algorithm. The response signal comprises this authentication code. The received authentication code is

then compared with an authentication code calculated in the same way on the apparatus' side of the air interface. Then the authenticity of the user is determined based on the comparison. Such a method provides excellent credibility.

Preferably in the method, the transponder may be intended to be used as an RFID-tag.

In accordance with a third aspect, the invention relates to a system for authenticating a user, carrying a portable, electronic device, comprising a transponder with a memory unit. The system comprises an interrogating apparatus and is characterised by means in the interrogating apparatus for transmitting a transponder interrogating signal to the transponder of the portable device; means in the interrogating apparatus for receiving a response signal, comprising user specific information, from the transponder, said user-specific information being written, by means in the portable, electronic device, into a memory unit of the transponder; and means for determining the authenticity of the user based on the user-specific information.

Such a system may operate in connection with or include a portable, electronic device and provides user-oriented authentication with high credibility.

Preferably in the system, the transponder interrogating signal comprises a request code, allowing the portable, electronic device to calculate an authentication code, to be transmitted by the transponder, the calculation being based on the request code and a user-specific key and using an algorithm. The response signal comprises the authentication code and the system comprises means for comparing the received authentication code with an authentication code calculated in the same way on the apparatus' side of the air interface. The system furthermore comprises means for determining the authenticity of the user based on the comparison. Such a system provides excellent credibility.

In a preferred embodiment, the transponder is intended to be used as an RFID-tag.

Brief description of the drawings

Fig 1 illustrates the basic concept of RFID-transponders.

Fig 2 shows a block diagram of a portable, electronic device according to an embodiment of the invention.

Fig 3a-3c illustrate embodiments of the invention with features for enhanced security.

Description of preferred embodiments

RFID tags (RFID= Radio Frequency Identification) or RFID transponders are information carriers widely used in modern technology. The well known basic concept of RFID transponders is illustrated by means of an example in Fig 1, wherein a transponder 101 (shown enlarged) is attached to an object 102, from which information is to be retrieved by means of an interrogating apparatus 103, sometimes referred to as a reading device.

The transponder 101 comprises an antenna 104 and an integrated circuit (IC) 105, which comprises a transponder memory unit. In order, for instance, to identify the object 102, the interrogating apparatus transmits a request radio signal 106, emitted as an electromagnetic field, which is picked up by the transponder antenna 104 and fed to the transponder IC 105. This causes the transponder 101 to transmit a reply signal 107 comprising information which is stored in the transponder memory unit in the IC 105. The information may be information identifying the object 102. Transmission is carried out using the transponder antenna 104. The reading device thus receives information from the transponder.

There are passive transponders and active transponders. Passive transponders have no internal power supply. Instead, passive transponders use the energy in

the received interrogating signal to create the reply signal. Active transponders on the other hand are provided with, or connected to, some kind power supply.

The transponder IC may be programmed with information in different ways. Information may be permanently embedded into the hardware when the IC is manufactured. It may also be fed to the IC using wires, or from an interrogating apparatus by means of the air interface. Hence, there are read-only as well as read/write transponders.

Transponder operating frequencies vary from 30 kHz (low-frequency transponders) to more than 2.5 GHz (high-frequency transponders). The stored information quantity varies from a few bytes (passive read-only transponders) up to 1MB (active read/write transponders). Reading ranges vary from a few centimetres to tens of metres.

An advantage with transponders compared with other information carriers, such as for instance bar codes, is that line-of-sight between reading device (interrogating apparatus) and information carrier (transponder) is not required. The time required to read a transponder is often less than 100 ms.

Fig 2 shows a block diagram of a portable, electronic device 201 according to an embodiment of the invention. In this embodiment, the device 201 is a GSM mobile telephone. When such a telephone is used, a SIM-module (SIM=Subscriber Identity Module), which is a detachable subscriber unit, is inserted into the phone. The SIM-module contains user-specific data and is accessible for the CPU (CPU=Central Processing Unit) of the telephone.

In this embodiment the telephone comprises an interface 204 between the CPU and the memory unit 203 of an RFID transponder 202 integrated into the telephone. This interface allows the telephone CPU to write user-specific information into the transponder memory unit 203 in the

transponder IC. Preferably, the interface 204 allows the CPU both to write information into the memory unit 203 and to read information from the memory. Moreover, it may be advantageous if the interface 204 allows the memory unit to provide interrupt signals to the CPU, for instance if the transponder has received an interrogating signal. In this embodiment the CPU retrieves the IMSI-number (IMSI=International Mobile Subscriber Identity) from the SIM-module. IMSI is a number with up to 15 digits that uniquely identify a subscriber and hence a user. The interface between the CPU and the transponder may be utilised by software-implemented functionalities, and may allow information to be transferred in both directions between the transponder and the CPU.

The SIM-module and the IMSI-number are standard features of GSM systems. Security may be enhanced by requiring a PIN-code for activating the SIM-unit (PIN=Personal Identification Number). The user-specific data (IMSI) may then be written into the memory unit as soon as the PIN-code has been entered.

The CPU is devised to write the IMSI-number or a code derived from the IMSI-number to the transponder memory unit. Upon interrogation, the transponder now transmits the IMSI-number, and hence user-specific information, to an interrogating apparatus.

If the identification procedure is associated with a payment, for instance the electronic payment of a bus ticket, this payment may preferably be effected via the users mobile telephony subscription.

The invention may be used extensively in connection with, for instance, vending machines, access control systems, movie theatres etc. Such services need then be provided with an interrogating apparatus, capable of contacting a device according to an embodiment of the invention. If a payment is involved as described above, the user may preferably be asked to acknowledge the payment in the user interface of the device before being provided

with the service (e.g. being let in at a movie theatre or a vending machine delivering goods).

Fig 3a-3c illustrate system embodiments of the invention with features for enhanced security. There is a risk that the transmission of the IMSI-number, as described in connection with fig 2, might be eavesdropped by a third party and may be misused by this party. In applications where this is critical, a more sophisticated approach may be considered.

GSM systems support features for authenticating a subscriber. These features involve a subscriber authentication key, Ki and an authentication algorithm A3. In GSM systems, the SIM-module, when provided with a 128 bit pseudo random number, referred to as RAND, calculates, based on Ki and RAND and using A3, a signed response, SRES. This allows the mobile telephony system to authenticate a subscriber. The algorithm A3 is designed so that it is extremely difficult to calculate Ki with RAND, SRES and A3 at hand. RAND may be referred to as a request code, whereas SRES may be referred to as an authentication code.

This functionality may be utilised in connection with an embodiment of the invention, as illustrated in fig 3a. Then in a method an interrogating apparatus (IA) emits a signal/field comprising a RAND-number. This signal is received by the transponder antenna and fed to the transponder IC. The CPU in the portable, electronic device reads the RAND number from the IC and feeds the number to the SIM unit. In the SIM unit an SRES (signed response) is calculated based on the RAND number, the Ki of the SIM unit, and using the A3-algorithm. The SRES is delivered to the CPU, which then writes SRES, being user-specific information, into the memory of the transponder IC. Subsequently, the transponder emits a signal containing SRES, which may be received by the interrogating apparatus. The interrogating apparatus may now check that the received SRES matches with an SRES, calculated in the

same way, but on the apparatus' side of the air-interface, between the transponder and the interrogating apparatus.

It should be noted that this embodiment may preferably be combined with the first embodiment, i.e. that both the IMSI-number and SRES may be delivered.

There are different ways for the interrogating apparatus to obtain a RAND and an SRES that is indicative for a given subscriber. As a first alternative the interrogating apparatus may generate a random number RAND and then generate SRES itself. This, however, requires that the interrogating apparatus has knowledge of the authentication key, Ki. Such keys are normally kept very secret, for instance only in the SIM unit and in a single server, such as the users HOME-MSC (MSC= Mobile Services Switching Centre). Therefore it is likely that the interrogating apparatus does not get access to the authentication key.

Instead, the interrogating apparatus may, as illustrated in fig 3b, generate RAND and request the corresponding SRES from such a server.

As an alternative, the interrogating apparatus may request, for a specific subscriber, a RAND and an SRES corresponding to this RAND. In order to use the correct authentication key, the server or interrogating apparatus, calculating the SRES, must know the identity of the subscriber. The interrogating apparatus may therefore, if the user identity is not already known, first obtain the user identity, for instance the IMSI-number, as described in connection with fig 2, and then perform authentication as described in connection with figs 3a-3c.

A third party, eavesdropping the IMSI, the RAND and the SRES, cannot authenticate himself as the subscriber vis-à-vis the interrogating apparatus, unless the interrogating apparatus uses the same RAND-number again, which is very unlikely (128 bit pseudo-random number, 2^{128} pos-

sibilities). Therefore, SRES may be regarded as a single-use code and excellent credibility is achieved.

The above example is related to the GSM-standard. The invention may also be used in connection with other types of mobile telephones, as long as user/subscriber-specific information is stored in the telephone.

The invention is however also useful in connection with other digital devices, such as for instance PDAs (PDA= Personal Digital Assistant). An RFID-transponder is then mounted in the PDA, and the PDA provides the transponder IC with user-specific information, which may be stored in the PDA or in a memory card inserted into the PDA.

It should also be noted that user-specific information may be manually entered into a portable, electronic device by using various user interfaces. A user may for instance enter a personal identity number or a subscriber number into a device, which number may then be used by the device to authenticate the user.

In summary, the invention relates to a portable, electronic device such as a mobile phone. The device is provided with a transponder and may be used for authentication purposes. The device includes means for writing user-specific information into a memory unit, connected with the transponder. Thus, when an interrogating reading device stimulates the transponder, the transponder emits the user-specific information. This enables authentication of a user rather than of a device. In a preferred embodiment use is made of a user-specific key, by means of which a single-use code is generated, which is used as the emitted user-specific information. The invention also relates to a method and a system, which may work in connection with such a device.

CLAIMS

1. Portable, electronic device (201) comprising a transponder (202) with a memory unit (203), c h a r a c t e r i s e d by means (204) for writing user-specific information into the transponder memory unit (203), so that the transponder (202), upon reception of an interrogating signal, generates a response signal comprising the user-specific information.

2. Portable, electronic device as claimed in claim 1, comprising a detachable subscriber unit (SIM) from which the user-specific information is retrieved.

3. Portable, electronic device as claimed in claim 1 or 2, comprising calculating means for calculating an authentication code (SRES), to be included in the user-specific information.

4. Portable, electronic device as claimed in claim 2 and 3, wherein the calculating means is located within the detachable subscriber unit (SIM).

5. Portable, electronic device as claimed in claim 3 or 4, wherein the authentication code (SRES) is calculated based on a user-specific key (Ki) and a request code (RAND) and using an algorithm (A3).

6. Portable, electronic device as claimed in claim 5, wherein the request code (RAND) is comprised in the interrogating signal, received by the portable electronic device.

7. Portable, electronic device as claimed in claim 2, wherein the user-specific information is a user identity number (IMSI).

8. Portable, electronic device as claimed in any one of the preceding claims, wherein the device is a mobile telephone.

9. Portable, electronic device as claimed in any one of the preceding claims, wherein the transponder is intended to be used as an RFID-tag.

10. Method for use in an interrogating apparatus for authenticating a user, carrying a portable, electronic device, comprising a transponder with a memory unit, c h a r a c t e r i s e d by the steps:

- transmitting a transponder interrogating signal to the transponder of the portable device;

- receiving a response signal, comprising user specific information, from the transponder, said user-specific information being written, by means in the portable, electronic device, into a memory unit of the transponder; and

- determining the authenticity of the user based on the user-specific information.

11. Method as claimed in claim 10, wherein the transponder interrogating signal comprises a request code (RAND), allowing the portable device to calculate an authentication code (SRES), to be transmitted by the transponder, the calculation being based on the request code (RAND) and a user-specific key (Ki) and using an algorithm (A3); wherein the response signal comprises the authentication code (SRES); wherein the received authentication code (SRES) is compared with an authentication code calculated in the same way on the apparatus' side of the air interface; and wherein the authenticity of the user is determined based on the comparison.

12. Method as claimed in any of claim 10 or 11, wherein the transponder is intended to be used as an RFID-tag.

13. System for authenticating a user, carrying a portable, electronic device, comprising a transponder with a memory unit, the system comprising an interrogating apparatus, c h a r a c t e r i s e d by

- means in the interrogating apparatus for transmitting a transponder interrogating signal to the transponder of the portable device;

- means in the interrogating apparatus for receiving a response signal, comprising user specific information,

from the transponder, said user-specific information being written, by means in the portable, electronic device, into a memory unit of the transponder; and

- means for determining the authenticity of the user based on the user-specific information.

14. System as claimed in claim 13, wherein the transponder interrogating signal comprises a request code (RAND), allowing the portable, electronic device to calculate an authentication code (SRES), to be transmitted by the transponder, the calculation being based on the request code (RAND) and a user-specific key (Ki) and using an algorithm (A3); wherein the response signal comprises the authentication code (SRES); where the system comprises means for comparing the received authentication code (SRES) with an authentication code calculated in the same way on the apparatus' side of the air interface; and wherein the system comprises means for determining the authenticity of the user based on the comparison.

15. System as claimed in claim 13 or 14, wherein the transponder is intended to be used as an RFID-tag.

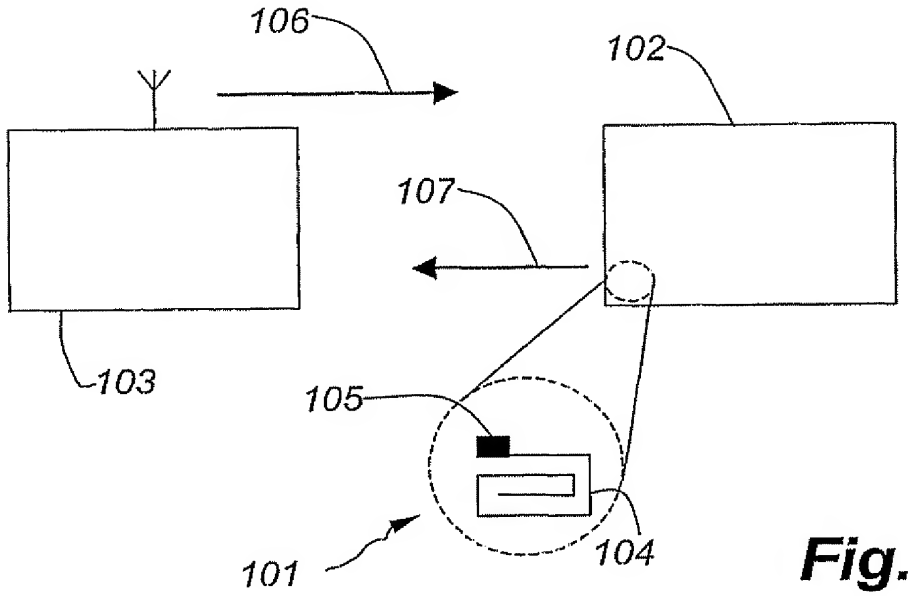
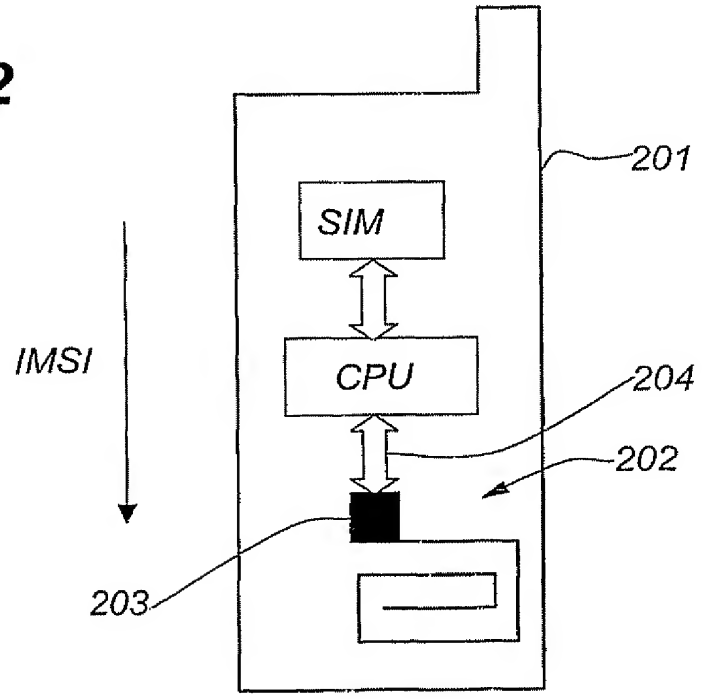


Fig. 1

Fig. 2



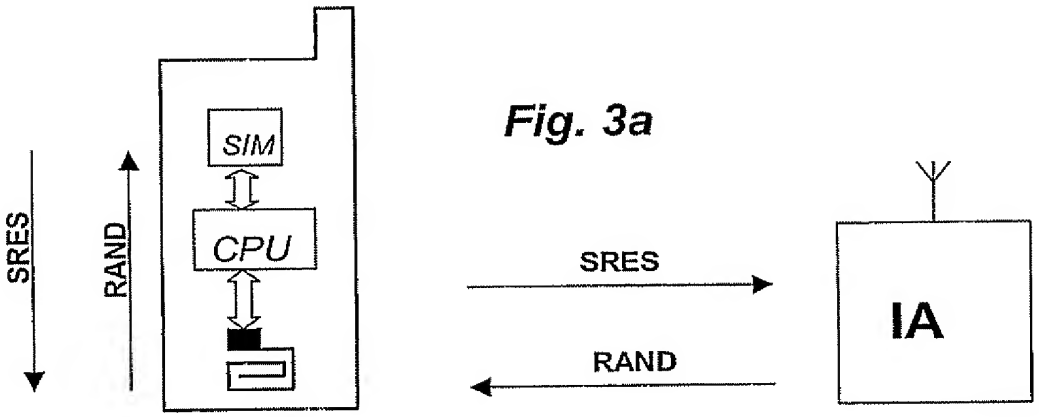


Fig. 3a

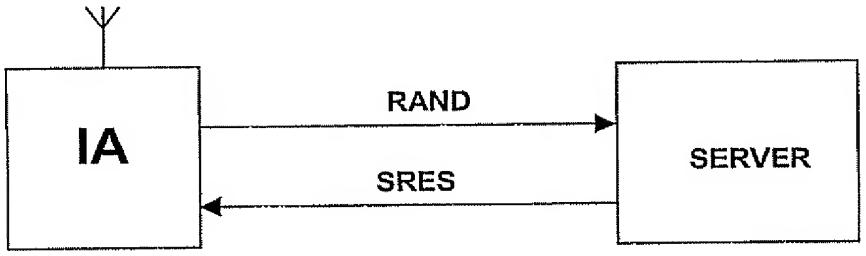


Fig. 3b

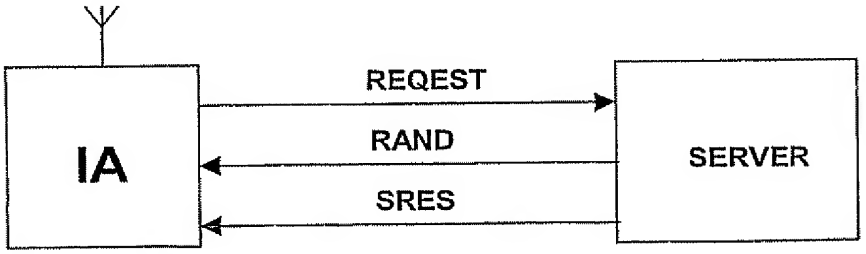


Fig. 3c

INTERNATIONAL SEARCH REPORT

Interni al Application No
PCT/IB 02/00911

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/38 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 02 11074 A (NOKIA MOBILE PHONES LTD ;ZALEWSKI THOMAS W (US); SHAW STEVEN A (US) 7 February 2002 (2002-02-07) page 5, line 8-11 page 11, line 3-6 page 11, line 20-26 abstract; claims 1,2 ---	1-15
Y	EP 1 005 244 A (ICO SERVICES LTD) 31 May 2000 (2000-05-31) column 2, line 35-43 abstract ---	1-15
Y	EP 0 828 354 A (ICO SERVICES LTD) 11 March 1998 (1998-03-11) column 13, line 38 -column 14, line 3 --- -/--	1-15

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 November 2002	29. 11. 2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	MALIN SÖDERMAN/JA A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Intern al Application No
PCT/IB 02/00911

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 201 12 099 U (MAYR ROLAND ;THATER DIRK (DE)) 18 October 2001 (2001-10-18) abstract	1-15
E	DE 102 02 015 A (RYL PETER ;SCHAURICH DIETER (DE)) 1 August 2002 (2002-08-01) abstract	1-15

INTERNATIONAL SEARCH REPORT

Intern l Application No
PCT/IB 02/00911

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 0211074	A	07-02-2002	AU	8082701 A	13-02-2002
			WO	0211074 A2	07-02-2002
EP 1005244	A	31-05-2000	EP	1005244 A1	31-05-2000
EP 0828354	A	11-03-1998	GB	2317074 A	11-03-1998
			EP	0828354 A2	11-03-1998
			JP	10155178 A	09-06-1998
			US	6324405 B1	27-11-2001
DE 20112099	U	18-10-2001	DE	20112099 U1	18-10-2001
DE 10202015	A	01-08-2002	DE	20100964 U1	28-02-2002
			DE	10202015 A1	01-08-2002